A. JOSEPH DeNUCCI
AUDITOR

The Commonwealth of Massachusetts

AUDITOR OF THE COMMONWEALTH
ONE ASHBURTON PLACE, ROOM 1819
BOSTON, MASSACHUSETTS 02108
TEL. (617) 727-6200

No. 2002-1105-4T

INDEPENDENT STATE AUDITOR'S REPORT
ON THE EXAMINATION OF
INFORMATION TECHNOLOGY-RELATED CONTROLS
AT THE MENTAL HEALTH LEGAL ADVISORS COMMITTEE

July 1, 2001 through February 28, 2002

OFFICIAL AUDIT REPORT
APRIL 15, 2002

2002-1105-4T

TABLE OF CONTENTS

INTRODUCTION

The Mental Health Legal Advisors Committee (MHLAC) is an agency within the Massachusetts Supreme Judicial Court. The MHLAC is mandated to secure and protect the rights of persons involved in mental health and retardation programs in the Commonwealth. The Mental Health Legal Advisors Committee is comprised of a total of fourteen judges and lawyers knowledgeable and experienced in mental health law. An Executive Director and five part-time staff members currently staff the MHLAC office.

The Mental Health Legal Advisors Committee's enabling legislation, mandated rules and the requirements of their regulations are stipulated through Massachusetts General Laws, Chapter 221, section 34E. The Committee's regulations are designed to ensure that legal representation is provided for individuals, families, and associations of people who by necessity are involved in the mental health system within the Commonwealth. In addition, the Committee advocates through the legislative process for the advancement of legal rights for mental health patients.

At the time of our audit, the primary information technology (IT) functions for MHLAC were supported through a file server and ten workstations configured as a local area network located at the Committee's office. The principle application systems available through the Committee's network were a case tracking system, Massachusetts Management Accounting and Reporting System (MMARS), and Microsoft office suite products. While each Committee staff member had access to application software for case tracking and the Microsoft office products, access to MMARS data was limited to the office manager.

The Office of the State Auditor's examination was limited to a review of certain IT general controls over and within the MHLAC's IT environment.

AUDIT SCOPE, OBJECTIVES AND METHODOLOGY

Audit Scope

From January 17, 2002 through March 14, 2002 we performed an information technology (IT) audit at the Mental Health Legal Advisors Committee covering the period of July 1, 2001 through February 28, 2002. Our audit scope included a review of IT-related general controls pertaining to organization and management, physical security, environmental protection, system access security, hardware and software inventory, business continuity planning, and on-site and off-site backup. Our review of logical access security was limited to access to the case tracking system installed on the Committee's local area network.

Audit Objectives

We sought to determine whether the Mental Health Legal Advisors Committee's IT-related internal control environment provided reasonable assurance that control objectives would be addressed to support business functions. We sought to determine whether IT organizational and management controls were in effect over data processing activities to ensure that such activities were managed effectively and efficiently and that IT policies and procedures were adequately documented and provided sufficient guidance for IT activities and functions. We sought to determine whether adequate physical security and environmental protection were in place to protect IT resources from unauthorized physical access and to safeguard the IT resources from damage or loss.

We sought to determine whether adequate controls were in place to prevent unauthorized system access to the case tracking system and related data files residing on the Committee's local area network. Our objective with respect to the Committee's hardware and software products was to determine whether adequate controls were in place and in effect to provide reasonable assurance that IT-resources were properly accounted for in an inventory record and were safeguarded against unauthorized use, theft, or damage.

Regarding system availability, we determined whether adequate controls were in place to provide reasonable assurance that on-site and off-site storage of backup media was in effect to assist recovery efforts and that IT processing and access to data files could be regained through a business continuity plan within an acceptable period of time should IT systems be rendered inoperable or inaccessible.

Audit Methodology

To determine the audit scope and objectives, we conducted pre-audit work that included obtaining and recording an understanding of relevant operations and reviewing documentation regarding MHLAC's mission, operations, and IT organization and management. We interviewed the Committee's Executive Director and staff to obtain an understanding of the Committee's operations and information technology control environment. In conjunction with our review of the internal control environment, we evaluated the degree to which the Committee had documented, authorized, and approved IT-related internal control policies and procedures for maintaining and monitoring cases through its case tracking system.

To accomplish a preliminary review of the adequacy of general controls over IT-related functions and assets, we obtained an understanding of and observed computer system operations, workstations and the file server at the Committee's office. To assess the adequacy of IT general controls, we interviewed MHLAC staff and performed selected audit tests.

Regarding our review of IT organization and management, we interviewed the Executive Director, requested documented IT policies and procedures and reviewed operational procedures and analyzed relevant documentation. To determine whether IT-related assets, including the file server, workstations, data files, and software, were adequately safeguarded from damage or loss, we reviewed physical security and environmental protection over IT resources through observation and interviews with the Committee's staff.

To assess the adequacy of controls to provide continued operations, we assessed the degree to which business continuity plans were required for the Committee and whether steps had been taken to implement recovery and contingency plans to regain essential operations should IT systems be rendered inoperable or inaccessible. In addition, we interviewed the Committee's staff to determine whether the criticality of application systems had been assessed, risks and exposures to computer operations had been evaluated, and a written and tested business continuity plan was in place. Further, we assessed the degree to which procedures required that copies of backup computer media would be generated and stored in secure on-site and off-site locations.

Our examination of system access security controls included a review of access privileges of those employees authorized to access the case tracking system. To determine whether existing system-based access privileges were authorized and were appropriate for current responsibilities, we reviewed procedures for granting and updating system access and reviewed granted privileges with respect to job responsibilities. To determine whether access security was being properly maintained through the management of user-IDs and passwords, we interviewed the Committee's staff and

compared the list of users to a list of Committee office personnel. We also determined whether procedures were in place to ensure that user-ID and passwords would be promptly deactivated from the system or the access privileges appropriately modified when staff had a change in personnel status (e.g., employment termination, job transfer, or leave of absence).

We conducted interviews and reviewed control documentation from the Committee to determine the adequacy of hardware and software inventory control policies and procedures. We obtained and reviewed an IT-related asset inventory record, which included hardware and software products. To determine whether the Committee's hardware inventory records were current, accurate, and valid, we performed a test of the inventory record, tracing all computer hardware inventory items from the list to the floor and reviewed the hardware items on the list for attributes including physical location, proper tagging, and condition. We also determined whether the Committee had conducted an annual physical inventory of fixed assets and reconciliation to the inventory record. In addition, we determined whether adequate controls were in place to provide reasonable assurance that LAN-based software would be properly accounted for by reviewing the inventory record.

Our audit was conducted in accordance with Generally Accepted Government Auditing Standards (GAGAS) of the United States and industry auditing practices. The audit criteria used for our control examination were based on applicable legal requirements and generally accepted IT control practices.

AUDIT SUMMARY

Based on our examination, we determined that controls in place provided reasonable assurance that control objectives pertaining to IT-related physical security, environmental protection, system access security, hardware and software inventory control, business continuity planning, and on-site and off-site backup of computer media would be met. However, our audit revealed that controls needed to be strengthened with regard to IT-related organization and management controls for documentation of IT policies and procedures.

Our review of IT-related organization and management disclosed that certain organizational controls were in place. Although the Committee had a small number of staff, we observed that compensating controls were in place to address control objectives requiring segregation of duties. Although we found the staff to be knowledgeable with respect to their responsibilities, certain IT-related policies and procedures were not formally documented. Specifically, we found that documentation of IT-related policies and procedures needed to be strengthened to provide sufficient operational rules, standards and guidelines to support operational and control objectives. We had found that there was little documentation of the policies and procedures that outlined operational and control objectives and IT management control practices with respect to logical access security, physical security, environmental protection, and hardware and software inventory control. In addition, we found that policies and procedures relating to business continuity planning needed to be enhanced.

We found that internal controls in place provided reasonable assurance of adequate physical security and environmental protection of the Committee's file server and ten workstations at their office location. With respect to physical security, personnel entering the building facility were subject to building security controls, and the office area was located in a secure area and would be staffed at the office entrance during business hours. We found that the Committee's office and the file server were located in securely locked areas. Our audit also revealed that there were adequate environmental protection controls in place, including smoke detectors, hand-held extinguishers, and an automatic fire-suppression system to protect IT-related assets.

Regarding system availability, MHLAC had developed a business continuity and disaster recovery plan. However, the Committee had not sufficiently documented its business continuity strategy or testing requirements to provide assurance of the recovery and contingency plan's viability. At the time of our audit, the Committee had not formalized an agreement with another agency for an off-site processing site. Although the recovery strategy appears to be adequate, the Committee needs to identify their alternate processing site, update their plan accordingly, and test the recovery and

contingency plan requirements for their viability. Importantly, the Committee needs to address the risks of not being able to recover within an acceptable period of time or incurring unnecessary data or system reconstruction costs.

Regarding backup of magnetic media, we found backup copies of magnetic media were being generated and stored on-site on a daily basis. However, we found that adequate environmental protection was not being afforded to on-site copies. According to the Committee, additional backup copies were being stored off-site on a weekly basis at a sister agency, however since we did not review the off-site storage location, we recommend that the Committee examine off-site storage for adequacy of physical security and environmental protection. Although the Committee had both on-site and off-site storage of computer media, the Committee should formally document all related procedures and establish mechanisms to assure proper physical security and environmental protection for storage of backup media to ensure that adequate resources for recovery would be available.

Regarding system access security, we found that system access controls provided reasonable assurance that only authorized users had access to the Committee's data files and programs residing on their local area network. We found that administrative controls over user-IDs and passwords provided reasonable assurance that access privileges would be deactivated or appropriately modified should the Committee's employees terminate employment or incur a change in job requirements. During the course of our audit, nothing came to our attention to indicate that there were weaknesses in access security to the Committee's case tracking system.

With respect to hardware and software inventory control, we found that the Committee, although not maintaining documented inventory policies and procedures, did have an inventory record delineating all of its hardware and software products. The inventory control procedures being exercised provided reasonable assurance that all IT-related assets were adequately listed, identified, and controlled, and our review of inventory items located in the Committee's office indicated that all of the items were locatable and properly accounted for. Although we noted that all items could be located, were in good condition, and were being utilized, we recommend that the Committee formalize procedures for tagging all the Committee's IT equipment and conduct an annual physical inventory to validate information on the inventory list. We found appropriate controls in place regarding the maintenance of the inventory record for software products and licenses.

AUDIT RESULTS

IT-related Organization and Management

Although our audit revealed that the MHLAC had certain IT-related general controls in place, control practices needed to be strengthened by having IT-related policies and procedures formally documented to provide sufficient guidance for performing IT-related functions and operations. Because IT operations are limited and are supported by office-based systems, the extent of required documentation for IT-related functions is not extensive. Although we acknowledge the Committee's difficulty in allocating limited staff resources to document IT-related policies and procedures, we believe that overall control practices would be strengthened by documenting policies and procedures regarding access security, physical security, environmental protection, hardware and software inventory control, and a comprehensive business continuity strategy.

Regarding its recovery strategy, the Committee needs to identify their alternate processing site, update their plan accordingly, review provisions and controls for off-site and on-site backup of computer media, and test the recovery and contingency plan requirements for their viability. Documented procedures might also cover information technology planning, risk assessment and risk management, definition of information architectures, data management for the case tracking system, virus protection, authorized use of IT resources, training, and monitoring and reporting. Although certain control practices and procedures were being performed with regard to some of these functions, written policies and procedures would help ensure that important operational and control objectives would be met.

Formal documentation of IT-related policies and procedures provides a sound basis for helping to ensure that desired actions are taken and that undesired events are prevented or detected and, if detected, that corrective action is taken in a timely manner. Documented policies and procedures also assist management in training staff and serve as a good basis for evaluation. They also enhance communication among personnel to improve operating effectiveness and efficiency. Clearly, formal documentation enables trained personnel to develop a broader understanding of their duties and improve their levels of competence.

In the absence of formal standards, policies and procedures, employees may rely on individual interpretations of what is required to be performed or how to best control IT-related systems and resources. In such circumstances, inconsistencies or omissions may result and key control objectives may not be adequately addressed. In addition, management may not be adequately assured that desired actions will be taken. Furthermore, the absence of documented policies and procedures

undermines the ability to monitor and evaluate IT operations and application systems because of the absence of stated internal controls and required audit or management trails. In addition to being a generally accepted control practice, Massachusetts General Laws, Chapter 647, requires that all state agencies have documented and approved internal control procedures.

Recommendation:

We recommend that the Mental Health Legal Advisors Committee begin documenting its IT-related policies and procedures to provide sufficient formal guidance to IT operations. Also, MHLAC should implement and strengthen its business continuity strategy and plan to help ensure system availability and resumption of IT operations within an acceptable time frame should processing be rendered inoperable or inaccessible.

Auditee's Response:

MHLAC accepts the recommendations of the audit and will begin a process of planning and implementation of these recommendations. The areas that MHLAC will focus on are:

- *Documentation of existing IT related policies and procedures;*
- *Improving and formalizing the MHLAC Business Continuity Plan.*

Documentation
MHLAC shall document its existing procedures and distribute to all staff formal written policies and procedures in the following areas – access security, physical security, environmental protection, inventory control, virus protection, authorized use of IT resources and data management for the case tracking system.

Business Continuity Plan
MHLAC will strengthen the Business Continuity Plan by making the arrangements to maintain the case tracking application in the same off-site location as the back up tape storage. Secondary, we will test the capacity to use the database and case tracking application off-site. Third, MHLAC will develop a protocol and train key staff in establishing operations off-site. MHLAC will evaluate effectiveness of the off-site storage.

The MHLAC will develop a work plan to complete implementation of these two recommendations by October 31, 2002.

MHLAC recognizes the importance of the internal control procedures set forth in the audit report and the need for additional monitoring and staff training. MHLAC will attempt to increase its related staff/consulting resources beyond current minimum levels in order to further enhance its IT controls. This will enable the Commonwealth to be assured that the investment in IT resources at MHLAC is adequately managed.

Auditor's Reply:

While understanding the budgetary constraints placed on your agency, we feel that the availability of IT systems and operational efficiency would be enhanced by documenting IT policies and procedures and a comprehensive business continuity strategy. We commend your measures to implement corrective action to our audit recommendations.